302 – SKYPE COMMUNICATIONS LOGS

TEAM INFORMATION

Team Name: AWGN

Results Email: [redacted]

Examination Time Frame: 10/21 to 10/25/08

INSTRUCTIONS

Description: Examiners must develop and document a methodology used to parse SKYPE communication logs from the communication/program files in the **302_SKYPE_Communications_Logs_Challenge2008** folder to an easily understandable, viewable, and readable rendering of the communications (remove non-conversation data). The supplied files were from either or both of the two computers used in the chat conversation. A detailed explanation of your process (software or technique) used to examine, extract, and present the data is required.

Points will be awarded for the completeness of the data recovered from the communications and the ease of understanding or utility of the method the information is reported from that file(s).

Total Weighted Points: 60 Total Points available per entry – Total 300 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

INTERNAL REVIEWER USE ONLY

Reviewer: Points Awarded:

Date: Review Period: to

Completed: ☐ Yes ☐ No ☐ Partial

Challenge Number: 301 - Encrypted Files and Folders

Examiner: Graham Eschbacher, Tim York

Conversation from D:\DC3\302_SKYPE_Communications_Logs_Challenge2008\2 yogibear1953
Message ID #kiki1932/$yogibear1953;422ef3cb540f2cc2

Wed Mar 05 20:38:21 2008 chatmsg256.dbb kiki1932 -> yogibear1953: hey, it's me, you there?
Wed Mar 05 20:39:01 2008 chatmsg256.dbb yogibear1953 -> kiki1932: yea, i'm here, what's up?
Wed Mar 05 20:52:51 2008 chatmsg256.dbb yogibear1953 -> kiki1932: hold on, got an important phone call. i'll get back with u
Wed Mar 05 20:52:51 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Ø¯kiki1932
Wed Mar 05 20:53:15 2008 chatmsg256.dbb kiki1932 -> yogibear1953: ok
Mon Mar 31 17:54:59 2008 chatmsg256.dbb yogibear1953 -> kiki1932: So Bob, what's happening, you haven't been on in awhile?
Mon Mar 31 17:55:24 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Sorry, been taking care of all the other business herer, didn't have the time.
Mon Mar 31 17:56:08 2008 chatmsg512.dbb yogibear1953 -> kiki1932: You know we still have that time thing going on, we miss our chance and we're out of luck this time, maybe for a long time
Mon Mar 31 17:56:16 2008 chatmsg512.dbb kiki1932 -> yogibear1953: you know, we shouldn't be using names int htis converstion and yea I know about the time thing but we gotta be careful man
Mon Mar 31 17:56:48 2008 chatmsg256.dbb yogibear1953 -> kiki1932: sorry didn't think about the name thing just nervous I guess
Mon Mar 31 17:56:55 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Jut think about what your going to do with all that money and youll feel better soon
Mon Mar 31 17:57:00 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Ok
Mon Mar 31 17:57:07 2008 chatmsg256.dbb kiki1932 -> yogibear1953: you got the weapons and other gear?
Mon Mar 31 17:57:49 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Yea, thought I was going to have a problem with the guns, by my uncle's a hunter and had a lot so I just "borrowed" some from him
Mon Mar 31 17:57:58 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Will he get wise?
Mon Mar 31 17:58:40 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Naw, he keps them in the basement and hasn't used them in years. they were in an old metal cabinet, dusty and dirty as all get out
Mon Mar 31 17:58:48 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Didn't leave any traces you were ther and took them out
Mon Mar 31 17:59:31 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Nope, used a rag over my nands and blew some dust back over where they had been sitting. Things were a pain to clean though
Mon Mar 31 17:59:42 2008 chatmsg256.dbb kiki1932 -> yogibear1953: How bout the ammo?
Mon Mar 31 17:59:57 2008 chatmsg256.dbb yogibear1953 -> kiki1932: I just went down and bought some new
Mon Mar 31 18:00:09 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Didn't have to give them a name or anything did you?
Mon Mar 31 18:00:17 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Nope, just like buying steaks at the grocery
Mon Mar 31 18:00:20 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Good, how bout the rest of the swtufff
Mon Mar 31 18:01:01 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Got an old can of black powder from his basement also, maybe 30 pounds, old but never been opened, should still be good
Mon Mar 31 18:01:04 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Didn't buy new
Mon Mar 31 18:01:37 2008 chatmsg512.dbb yogibear1953 -> kiki1932: They would have wanted ID for that man, and I only have the one fake set and I didn't want to burn it on that
Mon Mar 31 18:01:46 2008 chatmsg512.dbb kiki1932 -> yogibear1953: Good, whit what I got out of the anarchists cookbook combined with that were going to open some eyesw I'll tell you that
Mon Mar 31 18:01:59 2008 chatmsg256.dbb yogibear1953 -> kiki1932: When we hit this place its going to be empty right?
Mon Mar 31 18:02:48 2008 chatmsg512.dbb kiki1932 -> yogibear1953: Except for some roving security and I told you I scoped that out and timed them up. Always taking lunc together at the same time so we got an hour
Mon Mar 31 18:02:49 2008 chatmsg512.dbb yogibear1953 -> kiki1932: I just don't want any mistakes. It's one thing to do this but murder, man they sick a needle in your arm and that stuff burning is the last thing you feel
Mon Mar 31 18:03:28 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Settle down. If we stick to the plan and do this right theyrll be no problems
Mon Mar 31 18:03:31 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Yea, that's what you say now, but that's not the way it worked out last time

Mon Mar 31 18:04:13 2008 chatmsg512.dbb kiki1932 -> yogibear1953: That was justt bad luck, and it was bad luck for them. I didn't want anyone to get hurt, you know that
Mon Mar 31 18:04:29 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Don't change a thing man, you still killed them
Mon Mar 31 18:04:56 2008 chatmsg512.dbb kiki1932 -> yogibear1953: Listen amigo you were right there too and unless you shut up and follwo the plan well both be looking a a ride on the needle SO SHUT YOUR MOUTH ABOUT THE LAST JOB
Mon Mar 31 18:05:32 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Don't talk to me that way. I've been loyal and haven't said a thing. I know they're still looking for who pulled that and that means us. I aint gonna help them kill me
Mon Mar 31 18:05:40 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Sorry, jut the pressure, I know you won't and didn't talk
Mon Mar 31 18:06:28 2008 chatmsg512.dbb kiki1932 -> yogibear1953: listen, we got this going and just need to chill awhile. Gotta get off this comm and get on the other one we set up so they cant trace us so good. Get up on that one, regular time and well finish the planning
Mon Mar 31 18:06:42 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Ok man, later
Mon Mar 31 18:06:48 2008 chatmsg256.dbb kiki1932 -> yogibear1953: later

Conversation from D:\DC3\302_SKYPE_Communications_Logs_Challenge2008\Skype 1\kiki1932
Message ID #kiki1932/$yogibear1953;422ef3cb540f2cc2

Sun Mar 02 13:59:10 2008 chatmsg256.dbb yogibear1953 -> kiki1932: So Bob, what's happening, you haven't been on in awhile?
Sun Mar 02 13:59:36 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Sorry, been taking care of all the other business herer, didn't have the time.
Sun Mar 02 14:00:18 2008 chatmsg512.dbb yogibear1953 -> kiki1932: You know we still have that time thing going on, we miss our chance and we're out of luck this time, maybe for a long time
Sun Mar 02 14:00:27 2008 chatmsg512.dbb kiki1932 -> yogibear1953: you know, we shouldn't be using names int htis converstion and yea I know about the time thing but we gotta be careful man
Sun Mar 02 14:00:58 2008 chatmsg256.dbb yogibear1953 -> kiki1932: sorry didn't think about the name thing just nervous I guess
Sun Mar 02 14:01:06 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Jut think about what your going to do with all that money and youll feel better soon
Sun Mar 02 14:01:11 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Ok
Sun Mar 02 14:01:19 2008 chatmsg256.dbb kiki1932 -> yogibear1953: you got the weapons and other gear?
Sun Mar 02 14:02:00 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Yea, thought I was going to have a problem with the guns, by my uncle's a hunter and had a lot so I just "borrowed" some from him
Sun Mar 02 14:02:10 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Will he get wise?
Sun Mar 02 14:02:50 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Naw, he keps them in the basement and hasn't used them in years. they were in an old metal cabinet, dusty and dirty as all get out
Sun Mar 02 14:03:00 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Didn't leave any traces you were ther and took them out
Sun Mar 02 14:03:42 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Nope, used a rag over my nands and blew some dust back over where they had been sitting. Things were a pain to clean though
Sun Mar 02 14:03:54 2008 chatmsg256.dbb kiki1932 -> yogibear1953: How bout the ammo?
Sun Mar 02 14:04:08 2008 chatmsg256.dbb yogibear1953 -> kiki1932: I just went down and bought some new
Sun Mar 02 14:04:21 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Didn't have to give them a name or anything did you?
Sun Mar 02 14:04:27 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Nope, just like buying steaks at the grocery
Sun Mar 02 14:04:32 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Good, how bout the rest of the swtufff
Sun Mar 02 14:05:11 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Got an old can of black powder from his basement also, maybe 30 pounds, old but never been opened, should still be good
Sun Mar 02 14:05:16 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Didn't buy new
Sun Mar 02 14:05:47 2008 chatmsg512.dbb yogibear1953 -> kiki1932: They would have wanted ID for that man, and I only have the one fake set and I didn't want to burn it on that
Sun Mar 02 14:05:57 2008 chatmsg512.dbb kiki1932 -> yogibear1953: Good, whit what I got out of the anarchists cookbook combined with that were going to open some eyesw I'll tell you that
Sun Mar 02 14:06:09 2008 chatmsg256.dbb yogibear1953 -> kiki1932: When we hit this place its going to be empty right?
Sun Mar 02 14:06:59 2008 chatmsg512.dbb kiki1932 -> yogibear1953: Except for some roving security and I told you I scoped that out and timed them up. Always taking lunc together at the same time so we got an hour
Sun Mar 02 14:07:00 2008 chatmsg512.dbb yogibear1953 -> kiki1932: I just don't want any mistakes. It's one thing to do this but murder, man they sick a needle in your arm and that stuff burning is the last thing you feel

Sun Mar 02 14:07:39 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Settle down. If we stick to the plan and do this right theyrll be no problems
Sun Mar 02 14:07:41 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Yea, that's what you say now, but that's not the way it worked out last time
Sun Mar 02 14:08:25 2008 chatmsg512.dbb kiki1932 -> yogibear1953: That was justt bad luck, and it was bad luck for them. I didn't want anyone to get hurt, you know that
Sun Mar 02 14:08:40 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Don't change a thing man, you still killed them
Sun Mar 02 14:09:07 2008 chatmsg512.dbb kiki1932 -> yogibear1953: Listen amigo you were right there too and unless you shut up and follwo the plan well both be looking a a ride on the needle SO SHUT YOUR MOUTH ABOUT THE LAST JOB
Sun Mar 02 14:09:43 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Don't talk to me that way. I've been loyal and haven't said a thing. I know they're still looking for who pulled that and that means us. I aint gonna help them kill me
Sun Mar 02 14:09:51 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Sorry, jut the pressure, I know you won't and didn't talk
Sun Mar 02 14:10:39 2008 chatmsg512.dbb kiki1932 -> yogibear1953: listen, we got this going and just need to chill awhile. Gotta get off this comm and get on the other one we set up so they cant trace us so good. Get up on that one, regular time and well finish the planning
Sun Mar 02 14:10:53 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Ok man, later
Sun Mar 02 14:10:59 2008 chatmsg256.dbb kiki1932 -> yogibear1953: later
Wed Mar 05 17:40:52 2008 chatmsg256.dbb kiki1932 -> yogibear1953: hey, it's me, you there?
Wed Mar 05 17:41:31 2008 chatmsg256.dbb yogibear1953 -> kiki1932: yea, i'm here, what's up?
Wed Mar 05 17:55:21 2008 chatmsg256.dbb yogibear1953 -> kiki1932: hold on, got an important phone call. i'll get back with u
Wed Mar 05 17:55:21 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Ø¨yogibear1953
Wed Mar 05 17:55:45 2008 chatmsg256.dbb kiki1932 -> yogibear1953: ok

Conversation from D:\DC3\302_SKYPE_Communications_Logs_Challenge2008\Skype2\yogibear1953
Message ID #kiki1932/$yogibear1953;422ef3cb540f2cc2

Wed Mar 05 20:38:21 2008 chatmsg256.dbb kiki1932 -> yogibear1953: hey, it's me, you there?
Wed Mar 05 20:39:01 2008 chatmsg256.dbb yogibear1953 -> kiki1932: yea, i'm here, what's up?
Wed Mar 05 20:52:51 2008 chatmsg256.dbb yogibear1953 -> kiki1932: hold on, got an important phone call. i'll get back with u
Wed Mar 05 20:52:51 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Ø¨kiki1932
Wed Mar 05 20:53:15 2008 chatmsg256.dbb kiki1932 -> yogibear1953: ok
Mon Mar 31 17:54:59 2008 chatmsg256.dbb yogibear1953 -> kiki1932: So Bob, what's happening, you haven't been on in awhile?
Mon Mar 31 17:55:24 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Sorry, been taking care of all the other business herer, didn't have the time.
Mon Mar 31 17:56:08 2008 chatmsg512.dbb yogibear1953 -> kiki1932: You know we still have that time thing going on, we miss our chance and we're out of luck this time, maybe for a long time
Mon Mar 31 17:56:16 2008 chatmsg512.dbb kiki1932 -> yogibear1953: you know, we shouldn't be using names int htis converstion and yea I know about the time thing but we gotta be careful man
Mon Mar 31 17:56:48 2008 chatmsg256.dbb yogibear1953 -> kiki1932: sorry didn't think about the name thing just nervous I guess
Mon Mar 31 17:56:55 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Jut think about what your going to do with all that money and youll feel better soon
Mon Mar 31 17:57:00 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Ok
Mon Mar 31 17:57:07 2008 chatmsg256.dbb kiki1932 -> yogibear1953: you got the weapons and other gear?
Mon Mar 31 17:57:49 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Yea, thought I was going to have a problem with the guns, by my uncle's a hunter and had a lot so I just "borrowed" some from him
Mon Mar 31 17:57:58 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Will he get wise?
Mon Mar 31 17:58:40 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Naw, he keps them in the basement and hasn't used them in years. they were in an old metal cabinet, dusty and dirty as all get out
Mon Mar 31 17:58:48 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Didn't leave any traces you were ther and took them out
Mon Mar 31 17:59:31 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Nope, used a rag over my nands and blew some dust back over where they had been sitting. Things were a pain to clean though
Mon Mar 31 17:59:42 2008 chatmsg256.dbb kiki1932 -> yogibear1953: How bout the ammo?
Mon Mar 31 17:59:57 2008 chatmsg256.dbb yogibear1953 -> kiki1932: I just went down and bought some new

Mon Mar 31 18:00:09 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Didn't have to give them a name or anything did you?
Mon Mar 31 18:00:17 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Nope, just like buying steaks at the grocery
Mon Mar 31 18:00:20 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Good, how bout the rest of the swtufff
Mon Mar 31 18:01:01 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Got an old can of black powder from his basement also, maybe 30 pounds, old but never been opened, should still be good
Mon Mar 31 18:01:04 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Didn't buy new
Mon Mar 31 18:01:37 2008 chatmsg512.dbb yogibear1953 -> kiki1932: They would have wanted ID for that man, and I only have the one fake set and I didn't want to burn it on that
Mon Mar 31 18:01:46 2008 chatmsg512.dbb kiki1932 -> yogibear1953: Good, whit what I got out of the anarchists cookbook combined with that were going to open some eyesw I'll tell you that
Mon Mar 31 18:01:59 2008 chatmsg256.dbb yogibear1953 -> kiki1932: When we hit this place its going to be empty right?
Mon Mar 31 18:02:48 2008 chatmsg512.dbb kiki1932 -> yogibear1953: Except for some roving security and I told you I scoped that out and timed them up. Always taking lunc together at the same time so we got an hour
Mon Mar 31 18:02:49 2008 chatmsg512.dbb yogibear1953 -> kiki1932: I just don't want any mistakes. It's one thing to do this but murder, man they sick a needle in your arm and that stuff burning is the last thing you feel
Mon Mar 31 18:03:28 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Settle down. If we stick to the plan and do this right theyrll be no problems
Mon Mar 31 18:03:31 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Yea, that's what you say now, but that's not the way it worked out last time
Mon Mar 31 18:04:13 2008 chatmsg512.dbb kiki1932 -> yogibear1953: That was justt bad luck, and it was bad luck for them. I didn't want anyone to get hurt, you know that
Mon Mar 31 18:04:29 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Don't change a thing man, you still killed them
Mon Mar 31 18:04:56 2008 chatmsg512.dbb kiki1932 -> yogibear1953: Listen amigo you were right there too and unless you shut up and follwo the plan well both be looking a a ride on the needle SO SHUT YOUR MOUTH ABOUT THE LAST JOB
Mon Mar 31 18:05:32 2008 chatmsg512.dbb yogibear1953 -> kiki1932: Don't talk to me that way. I've been loyal and haven't said a thing. I know they're still looking for who pulled that and that means us. I aint gonna help them kill me
Mon Mar 31 18:05:40 2008 chatmsg256.dbb kiki1932 -> yogibear1953: Sorry, jut the pressure, I know you won't and didn't talk
Mon Mar 31 18:06:28 2008 chatmsg512.dbb kiki1932 -> yogibear1953: listen, we got this going and just need to chill awhile. Gotta get off this comm and get on the other one we set up so they cant trace us so good. Get up on that one, regular time and well finish the planning
Mon Mar 31 18:06:42 2008 chatmsg256.dbb yogibear1953 -> kiki1932: Ok man, later
Mon Mar 31 18:06:48 2008 chatmsg256.dbb kiki1932 -> yogibear1953: later

Methodology / Notes Form

Challenge Number: 302 - SKYPE Communications Logs

Tool Information

Type	Name	Publisher
○ Commercial ◉ Open Source	Python	Python Software Foundation www.python.org
○ Commercial ○ Open Source		
○ Commercial ○ Open Source		
○ Commercial ○ Open Source		
○ Commercial ○ Open Source		

Notes

A quick Google search for Skype Log analysis provided a nice pdf from www.lpcforensic.it/public_html/yabbfiles/Attachments/SkypeLogFileAnalysis.pdf that gave insight to the different headers located within each log file. Because conversation data is the desired result, only chatmsg256.dbb and chatmsg512.dbb were analyized (for each set of logs).

A Python (version 2.6) script was written to parse these files and extract the records. At the minimum, a record contains a time stamp, message ID, the username of the sender, and the sender's display name. It could also contain several messages (observed at most 2) containing the actual conversation. This script can output the log information according to each file name, or it displays the conversation, spanning multiple files and sorted by time stamp, separating conversations for differing message IDs. By default, conversation style is used, and is hard-coded in the script. It lists the time stamp, the file in which it was found, the direction of the message, and the message.

The following is the command used to parse the logs given in the 3 directories (run from the script directory; Relative paths also work):

python 302_parse_chatmsg.py conversation.txt "D:\DC3\302_SKYPE_Communications_Logs_Challenge2008\2 yogibear1953" "D:\DC3\302_SKYPE_Communications_Logs_Challenge2008\Skype2\yogibear1953" "D:\DC3\302_SKYPE_Communications_Logs_Challenge2008\Skype 1\kiki1932"